Claims:

1-19. (Cancelled)

20. (Withdrawn) A method for managing digital rights, the method comprising:

detecting a data file on a user device;

identifying the data file using a file recognition algorithm;

searching for information relating to an authorization to access the data file using data stored in a non-volatile storage area of the user device; and

allowing access to the data file if an authorization to access the data file is found during the search.

21. (Withdrawn) The method of claim 20 wherein the file recognition algorithm comprises a digital fingerprinting detection technique.

22. (Withdrawn) The method of claim 20 wherein the data file comprises a media file.

23. (Withdrawn) The method of claim 20 wherein the search for information relating to an authorization to access the data file is conducted in a license database on the user device.

24. (Withdrawn) The method of claim 23 wherein the data stored in a non-volatile storage area of the user device identifies a location of the license database in a volatile storage area of the user device.

25. (Withdrawn) The method of claim 20 wherein the search for information relating to an authorization to access the data file is conducted in a license database associated with a remote server.

26. (Withdrawn) The method of claim 20 further comprising:

offering for purchase an authorization to access the data file;

receiving an acceptance of the offer to purchase; and

allowing access to the data file in response to the acceptance of the offer.

27. (Withdrawn) The method of claim 26 further comprising storing information relating to an authorization to access the data file in a database on the user device in response to the acceptance of the offer to purchase.

28. (Withdrawn) The method of claim 20 further comprising applying a digital wrapper to the data file, with the digital wrapper associated with the identified file.

29. (Withdrawn) A method for allocating proceeds in connection with a distribution of digital rights, the method comprising:

receiving a data file on a user device, wherein the data file includes a digital wrapper including information relating to at least one distributor of the data file;

receiving a request to purchase a right to access the data file;

extracting the information relating to at least one distributor from the digital wrapper; and

allocating credits to the at least one distributor based on the extracted information.

30. (Withdrawn) The method of claim 29 wherein the digital wrapper further includes information relating to an assigned allocation of royalties associated with purchases of rights to access the data file.

31. (Withdrawn) The method of claim 30 wherein the extracted information comprises a unique file identifier, the method further comprising retrieving at least one of the distributor information or the royalty allocation information using the unique file identifier.

32. (Withdrawn) The method of claim 31 wherein the retrieved information is retrieved from a central database located remotely from the user device.

33. (Withdrawn) The method of claim 29 further comprising sending the request to purchase to a central server and storing the allocation of credits in a database associated with the central server.

34. (Withdrawn) A method for allocating proceeds in connection with a distribution of digital rights, the method comprising:

receiving a data file on a user device, wherein the data file includes a digital wrapper including information relating to one or more distributors of the data file;

identifying a user of the user device;

modifying the digital wrapper to include information relating to the identification of the user, wherein a detection of the data file with the modified digital wrapper enables an allocation of credit to the user.

35. (Withdrawn) The method of claim 34 wherein the digital wrapper is adapted to prevent access to the data file without a valid authorization.

36. (Withdrawn) The method of claim 35 further comprising:

sending the data file with the modified digital wrapper to a device associated with a consumer;

receiving a request to purchase access to the data file from the consumer device; and

disabling the digital wrapper on the consumer device in response to the received request.

37. (Withdrawn) The method of claim 36 further comprising allocating credit for the consumer purchase among the one or more distributors.

38. (Withdrawn) The method of claim 34 wherein the information relating to the identification of the user comprises a unique user identifier for the user, with the unique user identifier assigned by a central server.

39. (Withdrawn) The method of claim 34 wherein the data file comprises a media file.

40. (Withdrawn) A method for facilitating digital rights management on a user device, the method comprising:

collecting information relating to a user device from the user device, with the information relating to the user device including unique identification data for the user device;

generating a digital key using the collected information;

storing the digital key;

encrypting the digital key;

sending the encrypted key to the user device for storage on the user device;

receiving, from the user device, the encrypted key and information relating to the user device; and

validating the user device using at least two components selected from the group consisting of the received encrypted key, the received information, and the stored digital key.

41. (Withdrawn) The method of claim 40 further comprising collecting identification information relating to a user of the user device, wherein the digital key is generated using the identification information relating to the user.

42. (Withdrawn) The method of claim 40 wherein the collected information is collected in accordance with executable code stored on the user device.

43. (Withdrawn) The method of claim 40 wherein the digital key is generated by and stored on a central server.

44. (Withdrawn) The method of claim 40 wherein validating the user device comprises:

decrypting the encrypted key; and

comparing the encrypted key to the stored digital key.

45. (Withdrawn) The method of claim 40 wherein validating the user device comprises:

generating a digital key using the received information relating to the user device; and

comparing the digital key to the stored digital key.

46. (Withdrawn) The method of claim 40 further comprising authorizing access to a license database in response to validating the user device.

47. (Withdrawn) The method of claim 40 further comprising authorizing access to a digital file in response to validating the user device.

48. (Withdrawn) The method of claim 40 wherein the unique identification data is extracted from a non-volatile storage area of the user device.

49. (Previously Presented) A method for managing digital rights, the method comprising:

monitoring an input/output system of a user device for attempted file transfers;

detecting an attempt to transfer a data file between the user device and an external device through one of the input/output ports of the user device, wherein the data file is stored in an unwrapped form prior to the attempt to transfer the data file; and

applying a digital wrapper to the unwrapped data file in response to the detected attempt to transfer the data file before allowing the attempted transfer, wherein the digital wrapper is adapted to prevent unauthorized access to the data file after the data file is transferred between the user device and the external device.

50. (Original) The method of claim 49 wherein the data file comprises a media file.

51. (Previously Presented) The method of claim 49 further comprising identifying the data file as embodying a particular protected work from a plurality of predetermined works, wherein the digital wrapper is applied based on the identity of the data file.

52. (Original) The method of claim 51 wherein the digital wrapper is applied based on the identity of the data file matching an identification of the data file in a database on the user device.

53. (Previously Presented) The method of claim 51 wherein identifying the data file comprises using a file recognition algorithm adapted for identifying data files as embodying particular protected works based on characteristics of the data files.

54. (Previously Presented) The method of claim 49 wherein the digital wrapper includes information identifying the data file and information relating to an allocation of credits to one or more distributors of the data file based on purchases of the data file.

55. (Withdrawn) A method for managing digital rights, the method comprising:

identifying a digital file on a first user device, wherein the digital file is subject to a license in accordance with license information stored on the first user device;

receiving a request to copy the digital file from the first user device to a second user device;

obtaining information associated with the second user device, including unique identification data for the second user device;

copying the digital file from the first user device to the second user device;

storing data on the first user device, wherein the data identifies the copied digital file and identifies the second user device.

56. (Withdrawn) The method of claim 55 further comprising synchronizing the stored data on the first user device with a central database.

57. (Withdrawn) The method of claim 55 further comprising determining that the requested copying of the digital file is authorized based on the license information.

58. (Withdrawn) The method of claim 57 wherein the license information is contained in a digital wrapper for the digital file.

59. (Withdrawn) The method of claim 55 further comprising storing the license information for the digital file on the second user device.

60. (Previously Presented) A method for managing digital rights, the method comprising:

identifying a media file stored on a user device for distribution to an external device, where the media file is stored in an unwrapped form prior to distribution;

identifying access rules associated with the media file, wherein the access rules include information relating to usage rights and usage fees;

applying a digital wrapper to the media file before distribution occurs, with the digital wrapper including identification data for the media file and data relating to the access rules, wherein the digital wrapper is adapted to prevent unauthorized access to the media file after the media file is distributed to the external device.

61. (Previously Presented) The method of claim 60 wherein the digital wrapper is adapted to be disabled for use of the media file by an external device that has a license to access the media file.

62. (Original) The method of claim 60 wherein the digital wrapper further includes information relating to at least one distributor of the media file.

63. (Withdrawn) A method for managing digital rights, the method comprising:

encoding a media file with licensing information;

locking the media file using a digital wrapper to prevent unauthorized access;

loading the wrapped media file onto a user device;

installing instructions on the user device to allow unlocking of media files, wherein the instructions provide for identifying the media file and sending a message, in accordance with the licensing information encoded in the media file, to a remote server to obtain a license to use the media file;

receiving a license to access the media file from the remote server; and

allowing access to the media file on the user device using the license.

64. (Withdrawn) The method of claim 63 further comprising storing the license to access the media file on the user device.

65. (Withdrawn) The method of claim 63 wherein the license includes data for unlocking the media file.

66. (Withdrawn) A system for managing digital rights, comprising:

a centralized database adapted to store identifiers for a plurality of digital files and adapted to store user licenses to use the digital files;

a centralized server operable to receive messages via a network from a remote device, with each received message including a user identifier for a user and identification information for a digital file, wherein the centralized server is further operable to process payment information for a license to use the digital file, to store information associating the license to use the digital file with the user, and to send licensing information for the digital file to the remote device; and

wherein the licensing information is adapted to enable the remote device to allow use of the digital file by the user.

67. (Withdrawn) The system of claim 66 wherein the centralized server is further operable to receive one or more digital keys from the remote device and to decrypt the one or more digital keys to validate an identity of at least one of the remote device or the user.

68. (Withdrawn) The system of claim 67 wherein the centralized server is further operable to receive device-specific data from the remote device for use in validating the remote device.

69. (Withdrawn) The system of claim 66 wherein the remote device comprises a server adapted to support streaming of digital files to a user device associated with the user.

70. (Withdrawn) The system of claim 69 wherein the remote device stores the licensing information.

71. (Withdrawn) The system of claim 66 wherein the remote device comprises a user device associated with the user.

72. (Withdrawn) The system of claim 71 wherein the centralized server is further adapted to receive information from the user device, generate a digital key associated with at least one of the user or the user device, and send the digital key to the user device, with the digital key being adapted to enable access to at least one of the license information, a license database containing the license information, or the digital file.

73. (Withdrawn) The system of claim 66 wherein the licensing information comprises data adapted for use in disabling a digital wrapper applied to the digital file.

74-84. (Cancelled)

85. (Withdrawn) An article comprising a machine-readable medium storing instructions for causing one or more processors to perform operations comprising:

detecting a data file on a user device;

identifying the data file using a file recognition algorithm;

searching for information relating to an authorization to access the data file using data stored in a non-volatile storage area of the user device; and

allowing access to the data file if an authorization to access the data file is found during the search.

86. (Withdrawn) The article of claim 85 wherein the machine-readable medium stores instructions for causing one or more processors to perform further operations comprising monitoring an input system of the user device, wherein detecting the data file occurs as a result of the monitoring.

87. (Withdrawn) The article of claim 86 wherein the data stored in the non-volatile storage area comprises a digital key for accessing a license database on the user device.

88. (Withdrawn) The article of claim 87 wherein the data stored in the non-volatile storage area comprises location information for the license database.

89. (Withdrawn) An article comprising a machine-readable medium storing instructions for causing one or more processors to perform operations comprising:

receiving information extracted from a digital wrapper applied to a data file, with the extracted information including an identification of the data file;

receiving a request to purchase an authorization to access the data file;

identifying at least one distributor of the data file based on the extracted information; and

allocating credits to the identified distributors in accordance with a predefined allocation structure.

90. (Withdrawn) The article of claim 89 wherein the extracted information includes an identifier associated with each of the identified distributors.

91. (Withdrawn) The article of claim 89 wherein allocating credits to the identified distributors is performed in accordance with data in the extracted information.

92. (Withdrawn) An article comprising a machine-readable medium storing instructions for causing one or more processors to perform operations comprising:

storing a data file on a user device, wherein the data file includes a digital wrapper including information relating to one or more distributors of the data file;

identifying a user of the user device;

modifying the digital wrapper to include information relating to the identification of the user, wherein a detection of the data file with the modified digital wrapper enables an allocation of credit to the user.

93. (Withdrawn) The article of claim 92 wherein the digital wrapper includes information relating to an assigned allocation of credit for the user.

94. (Withdrawn) The article of claim 92 wherein the digital wrapper is operable to prevent access to the data file without a valid authorization to access the data file.

95. (Withdrawn) An article comprising a machine-readable medium storing instructions for causing one or more processors to perform operations comprising:

receiving information relating to a user device from the user device, with the received information including unique identification data for the user device;

generating a digital key using the received information;

storing the digital key;

encrypting the digital key;

sending the encrypted key to the user device for storage on the user device

receiving, from the user device, the encrypted key and collected information relating to the user device, with the collected information being collected by the user device in accordance with instructions stored on the user device; and

validating the user device using at least two data items selected from the group consisting of the received encrypted key, the collected information, and the stored digital key.

96. (Withdrawn) The article of claim 95 wherein the machine-readable medium stores instructions for causing one or more processors to perform further operations comprising:

receiving from the user device a request for an authorization to access a data file; and

sending the authorization to access the data file in response to validating the user device.

97. (Withdrawn) The article of claim 96 wherein the encrypted key and the collected information is received in connection with the request for the authorization.

98. (Withdrawn) The article of claim 96 wherein the machine-readable medium stores instructions for causing one or more processors to perform further operations comprising storing an indication of the authorization to access the data file in response to validating the user device.

99. (Withdrawn) The article of claim 95 wherein the machine-readable medium stores instructions for causing one or more processors to perform further operations comprising:

receiving a unique identifier for a user associated with the user device; and

generating the digital key further using the unique identifier for the user.

100. (Previously Presented) An article comprising a machine-readable medium storing instructions for causing one or more processors to perform operations comprising:

monitoring an input/output system of a user device for attempted file transfers between the user device and an external device through one or more input/output ports of the user device;

detecting an attempt to transfer a data file between the user device and an external device through one of the input/output ports of the user device, wherein the data file is stored in an unwrapped form prior to the attempt to transfer the data file; and

applying a digital wrapper to the unwrapped data file in response to the detected attempt to transfer the data file before allowing the attempted transfer, wherein the digital wrapper is adapted to prevent unauthorized access to the data file after the data file is transferred between the user device and the external device.

101. (Original) The article of claim 100 wherein the machine-readable medium stores instructions for causing one or more processors to perform further operations comprising identifying the data file as being subject to protection from unauthorized copying.

102. (Original) The article of claim 101 wherein identifying the data file as being subject to protection from unauthorized copying includes locating an identifier for the data file in a database stored on the user device.

103. (Original) The article of claim 101 wherein identifying the data file as being subject to protection from unauthorized copying includes:

sending a message including information for identifying the data file to a remote server; and

receiving a response to the message indicating that the data file is subject to protection from unauthorized copying.

104. (Withdrawn) An article comprising a machine-readable medium storing instructions for causing one or more processors to perform operations comprising:

identifying a digital file on a first user device, wherein the digital file is subject to a license in accordance with license information stored on the first user device;

receiving a request to copy the digital file from the first user device to a second user device;

obtaining information associated with the second user device, including unique identification data for the second user device;

copying the digital file from the first user device to the second user device;

storing data on the first user device, wherein the data identifies the copied digital file and identifies the second user device.

105. (Withdrawn) The article of claim 104 wherein the machine-readable medium stores instructions for causing one or more processors to perform further operations comprising confirming that copying of the digital file to the second user device is permissible in accordance with the license information.

106. (Withdrawn) The article of claim 104 wherein receiving the request to copy the digital file comprises receiving an indication of an attempt to copy the digital file through a file output system of the first user device.

107. (Withdrawn) The article of claim 104 wherein the machine-readable medium stores instructions for causing one or more processors to perform further operations comprising sending the data to a remote server.

108. (Previously Presented) An article comprising a machine-readable medium storing instructions for causing one or more processors to perform operations comprising:

identifying a media file stored on a user device for distribution to an external device, where the media file is stored in an unwrapped form prior to distribution;

identifying access rules associated with the media file, wherein the access rules include information relating to usage rights and usage fees;

applying a digital wrapper to the media file before distribution occurs, with the digital wrapper including identification data for the media file and data relating to the access rules, wherein the digital wrapper is adapted to prevent unauthorized access to the media file after the media file is distributed to the external device.

109. (Original) The article of claim 108 wherein identifying the media file comprises identifying the media file using a file recognition algorithm.

110. (Original) The article of claim 108 wherein identifying the access rules associated with the media file comprises receiving access rules from a remote server.

111. (Previously Presented) The article of claim 108 wherein the machine-readable medium stores instructions for causing one or more processors to perform further operations comprising:

receiving a request from a user of the external device for authorization to access the media file after distribution of the media file from the user device;

notifying a remote server of the request for authorization to access the media file by the external device; and

disabling the digital wrapper to allow access to the media file by the user of the external device.

112. (Previously Presented) The article of claim 108 wherein identifying the access rules associated with the media file comprises receiving the access rules from the user device.

113. (Withdrawn) An article comprising a machine-readable medium storing instructions for causing one or more processors to perform operations comprising:

receiving a digital key;

storing the digital key in a non-volatile memory;

storing license information for at least one digital file in a license database in a volatile storage area;

identifying an attempt to access a specific digital file; and

allowing access to the digital file using the digital key if the license database includes license information identifying a license to the specific digital file.

114. (Withdrawn) The article of claim 113 wherein the digital key comprises data specific to a user device and the machine-readable medium stores instructions for causing one or more processors to perform further operations comprising:

retrieving identification information from the user device; and

validating the digital key using the identification information and the data specific to the user device.

115. (Withdrawn) The article of claim 113 wherein the digital key comprises location data for the license database and the machine-readable medium stores instructions for causing one or more processors to perform further operations comprising accessing the license database using the location data from the digital key.

116. (Withdrawn) The article of claim 113 wherein the machine-readable medium stores instructions for causing one or more processors to perform further operations comprising preventing access to the digital file if the license database does not include license information identifying a license to the specific digital file.

117. (Withdrawn) The article of claim 113 wherein the digital key comprises data necessary to decrypt at least one of the license database or the license information.

118. (Withdrawn) The article of claim 113 wherein the license information includes data necessary to disable a digital wrapper applied to the specific digital file.